

TecnetSOC vs. Vicarius

Vicarius is a tool your team operates. TecnetSOC is the service that runs your security for you, 24/7.

With Vicarius, your team builds groups, rules, and reports, is accountable for timelines, and needs its own EDR and SIEM; no one from the vendor watches your environment. **TecnetSOC is a service: the SOC patches, with critical patches in 48 hours as a target.**



43

capabilities where TecnetSOC goes further

7

capabilities where we match

0

capabilities where Vicarius outperforms TecnetSOC

Of the 50: 43 where we go further and 7 where we match

Same list of 50 capabilities and same criteria for TecnetSOC and Vicarius: each one's most complete published offering, with the source for every data point. [How we did it](#)

[Request the 30-day Response trial](#)

[or start free with Visibility, up to 10 devices](#)

tecnetone.com/en/services/soc-as-a-service

- ✓ 24/7 agentic SOC in LATAM, the US, and Europe
- ✓ Native Spanish and multilingual support
- ✓ Human Gate on critical actions
- ✓ ISO/IEC 27001:2022 certified operations
- ✓ Critical: notification and investigation start within 30 min (target)

Public information reviewed as of September 29, 2026. Version 2026.09. Informational comparison prepared by TecnetOne, not affiliated with the brands mentioned.

— BEFORE YOU COMPARE

Vicarius is a vulnerability remediation tool that your team operates; it is not a managed SOC service. Everything else you would need (EDR, SIEM, RMM, and backup) is purchased and operated separately, and not all of it integrates natively. This comparison shows, capability by capability, how much of what TecnetSOC includes Vicarius covers on its own and what you would have to add in products, contracts, and staff.

— WHAT SETS US APART

Differences you notice day to day

01

You buy software, you operate it

WITH VICARIUS

You buy a platform: your team creates groups, reports, and automations for each customer, based on its requirements and service level agreements (SLAs), and maintains them. [1]

WITH TECNETSOC

You purchase a service: TecnetOne's own analysts operate 24/7, and the SOC carries out patching, not your team.

02

No one is watching at 3 a.m.

WITH VICARIUS

There are no vendor analysts watching your environment: it's remediation software, and its team steps in after the incident to recover and harden. [2]

WITH TECNETSOC

Analysts in your time zone operate 24/7; for critical incidents, notification and investigation start within 30 minutes, as a target.

03

EDR and SIEM are on you

WITH VICARIUS

You need your own EDR and your own SIEM: the platform takes their signals without replacing either one, and each is licensed and operated separately. [3]

WITH TECNETSOC

The most complete plan includes EDR/XDR on every device and SIEM with MITRE ATT&CK correlation, operated by the SOC.

04

The patching timeline is yours

WITH VICARIUS

You choose to patch on demand, by window, or by rule; the vendor doesn't publish installation timelines, and meeting them depends on your team. [4]

WITH TECNETSOC

The SOC applies patches with written targets: critical in 48 h, important in 7 days, routine in 30 days, within your windows.

05

Email, identity, and network: not covered

WITH VICARIUS

You cover vulnerabilities and patches; email, phishing, identities, the internal network, and the external attack surface are left out, and each one requires another product and another console. [3]

WITH TECNETSOC

The most complete plan adds email security, phishing simulations, identity, NDR, and external attack surface in one service.

06

Mexican regulations, off the map

WITH VICARIUS

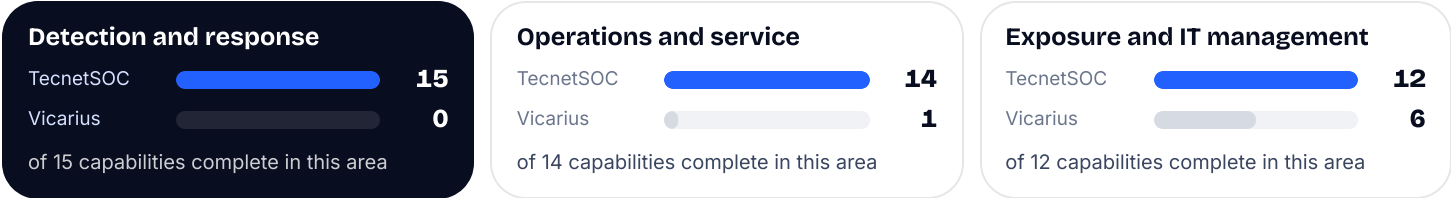
Remediation is mapped to frameworks such as NIST, CIS, and ISO 27001; CNBV, LFPDPPP, or NOM-024 don't appear, and it isn't presented as a GRC platform. [5]

WITH TECNETSOC

The TecnetGRC add-on (at an additional cost, purchased per standard) covers ISO 27001, SOC 2, PCI DSS, CNBV, LFPDPPP, and NOM-024 with an auditor portal.

— WHERE THE DIFFERENCE LIES

The three areas with the biggest gap



— CAPABILITY BY CAPABILITY

TecnetSOC and Vicarius, side by side

Capability	TecnetSOC	Vicarius Remediation	Evidence on Vicarius
✓ Offers it ✗ Not part of its published offering	⊕ Offers it as an add-on ● Your team provides it	Ⓢ Partial, limited, or requires another contract	❓ No public evidence
Operations and service	14 of 14	1 complete +2 partial	
24/7 security operations center (SOC) with human analysts	✓	Your team provides it	Software operated by the IT provider; not a SOC or MDR [3]
AI agents that investigate and filter alerts before passing them to an analyst	✓	✗	Its AI prioritizes vulnerabilities and generates scripts; it doesn't investigate alerts [6]
Human Gate: a person approves every critical action before it runs	✓	✗	No service with human approval; the IT provider configures remediation [7]

Capability	TecnetSOC	Vicarius Remediation	Evidence on Vicarius
☒ Offers it ☒ Offers it as an add-on ☒ Partial, limited, or requires another contract ☐ No public evidence			
☐ Not part of its published offering ☐ Your team provides it			
AI investigation assistant in the portal that cites its sources	☒ Neo	☐	No on-call AI analyst in the portal [3]
Operations in LATAM, the US, and Europe, with analysts in your time zone	☒	Your team provides it	No visible LATAM operations or focus [3]
Analysts, support, and portal in native Spanish	☒	☐	Support and materials in English [3]
Leadership reports in Spanish and in business language	☒	☐	Technical dashboards in English, not business reports in Spanish [8]
Published notification and investigation start times by severity	☒ Critical: 30 min (target)	Your team provides it	No notification commitments by severity; it isn't a service [3]
Executive summary every morning: what happened in the last 24 hours	☒ 7:30 a.m.	Your team provides it	No daily executive summary [3]
Automated weekly, monthly, quarterly, and annual reports	☒	☒	Tool reports; automated cadences not confirmed [8]
Assigned technical account manager (TAM) and quarterly reviews	☒	Your team provides it	No published TAM or quarterly reviews [3]
24/7 contact with support or security staff	☒	☐	No public evidence of 24/7 support [3]
Independent certification of operations (ISO 27001 or SOC 2 Type II)	☒ ISO/IEC 27001:2022	☒	States SOC 2 Type II; no published ISO 27001 certification of its own [9]
Fast start with a software agent: your devices' activity, visible within hours	☒ Typical: 2 to 4 hours	☒	SaaS with a fast-deploying agent; no published onboarding time [3]
Detection and response	15 of 15	0 complete	
		+2 partial	
Continuous monitoring and event correlation (SIEM), aligned with MITRE ATT&CK (a reference framework of attack techniques)	☒	☐	Not a SIEM [3]
Advanced protection on every device (EDR/XDR): malware, ransomware, and vulnerability exploitation	☒	☒	vShield protects in memory against exploitation; not an EDR or anti-malware [10]
Web filtering on the device	☒	☐	No web filtering [3]
Intrusion detection (IDS/IPS)	☒	☐	No IDS/IPS [3]
Threat detection on the internal network (NDR)	☒	☐	No NDR [3]
Documented investigations enriched with threat intelligence	☒	☐	Intelligence applied to vulnerabilities, not to incident investigation [6]
Incident management with a case log and response time measured per case	☒	☐	No incident management [3]
Response with device isolation and IP address blocking	☒	☐	No device isolation or IP blocking [3]
Incident response with root cause analysis	☒	Your team provides it	No incident response or forensics [3]
Identity posture: MFA, privileged accounts, and conditional access	☒	☐	No identity posture [3]
Zero Trust: secure DNS, application access, and control of unauthorized applications (shadow IT)	☒	☐	No Zero Trust [3]
Cloud security: alerts and posture	☒	☐	No Azure security [3]
Email security: spam, phishing, malware, and impersonation fraud (BEC)	☒	☐	No email security [3]
Security awareness: phishing simulations and training with metrics	☒	☐	No security awareness [3]

Capability	TecnetSOC	Vicarius Remediation	Evidence on Vicarius
☒ Offers it ☒ Offers it as an add-on ☒ Partial, limited, or requires another contract ☐ No public evidence			
☐ Not part of its published offering ☐ Your team provides it			
Prioritized security recommendations with an approval workflow	☒	☒	Remediation queue prioritized by vScore; no documented approval workflow [6]
Exposure and IT management	12 of 12	6 complete +0 partial	
Unified asset and software inventory	☒	☒	Agent-based asset and application inventory [11]
Vulnerabilities prioritized by severity and likelihood of exploitation (CVSS, EPSS)	☒	☒	vScore combines CVSS, EPSS, KEV, and asset context [12]
Priority for flaws already being exploited (CISA KEV catalog)	☒	☒	Uses the CISA KEV catalog in prioritization [12]
Operating system and third-party application patching	☒	☒	vPatch: OS and thousands of third-party apps (Vicarius figure) [7]
Provider-operated patching, with published timelines by severity	☒ Critical: 48 h (target)	Your team provides it	The IT provider carries out patching; no published times [3]
Closure verification: the scanner confirms the vulnerability is gone	☒	☒	Revalidates each fix and confirms the vulnerability is gone [13]
Patch validation in a pilot group before rollout	☒	☒	Asset groups to test remediations before general rollout [8]
External attack surface: what your company exposes on the internet, with a risk score	☒ Score from 0 to 100	☐	Factors internet exposure into the score; no EASM or external score [14]
Alerts for domains that imitate your brand and for exposed credentials or keys	☒	☐	No alerts for lookalike domains or exposed secrets [3]
Annual penetration test (pentest)	☒ Annual	Your team provides it	No pentesting [3]
Remote monitoring and management (RMM)	☒	☐	Not an RMM [3]
Uptime monitoring (NOC)	☒	☐	No uptime monitoring or NOC [3]
Backup and continuity	3 of 3	0 complete +0 partial	
Backup for servers, files, databases, virtual machines, and Microsoft 365	☒ Add-on	☐	No backup [3]
Immutable backup vault (cannot be altered or deleted), isolated per customer	☒ Add-on	☐	No immutable vault [3]
Disaster recovery with drills and measured recovery time (RTO)	☒ Add-on Measured RTO	☐	No disaster recovery [3]
Compliance	6 of 6	0 complete +2 partial	
Monthly evidence ready for auditors and insurers	☒ Monthly	☒	vComply generates CIS, PCI DSS, HIPAA, and CMMC reports; no comprehensive monthly evidence [5]
Readiness for ISO 27001, SOC 2, and PCI DSS with shared controls	☒ Add-on	☒	Maps vulnerability controls to frameworks; not a GRC platform [5]
Mexican regulatory readiness: CNBV Fintech, data protection (LFPDPPP), and NOM-024	☒ Add-on	☐	No Mexican regulations [3]
Risk management, controls, statement of applicability, and internal audits	☒ Add-on	☐	No risk management, SoA, or internal audits [3]
Auditor portal with an evidence room and a public trust page (trust center)	☒ Add-on	☐	Has its own Trust Center, not for the IT provider's customers [9]
Business continuity, vendor risk, and data breach management	☒ Add-on	☐	No continuity, vendor, or breach management [3]

Capability	TecnetSOC	Vicarius Remediation	Evidence on Vicarius
☒ Offers it ☒ Offers it as an add-on ☐ Partial, limited, or requires another contract ☐ No public evidence ☒ Not part of its published offering ☐ Your team provides it			
How it's purchased	Not counted		
Per-device pricing, with plans that stack	☒ Per device	☐	Per asset with a custom quote; no published stackable plans [15]
Free plan to get started	☒ Up to 10 devices	☒	No permanent free plan [16]
Free trial in your real environment	☒ 30 days	☐	Offers a free trial; duration not published [17]
Available under your IT provider's brand	☒	☒	Multi-tenant console and partner program; no documented white labeling [18]
Full coverage	50	7 +6 partial	

What your team would have to provide to run it 24/7: people, shifts, response times, a daily summary, incident response, and operated patching. TecnetSOC includes them in the service.

— NEXT STEP

From tool to service, with no implementation project

You install a single agent, see your devices' activity within hours, and our analysts operate 24/7 in your language.

The first agentic SOC in Spanish: platform, analysts, and support.

Request the 30-day Response trial

Start free with Visibility (up to 10 devices)

Or talk to a specialist

tecnetone.com/en/services/soc-as-a-service

HOW THE RESPONSE TRIAL WORKS

1

You install a single agent

2

You get the executive summary every morning

3

You decide with data from your environment

— APPENDIX

Methodology and sources

Who prepared it and how

We prepared it at TecnetOne and show you the source for every data point. The list of capabilities is based on the TecnetSOC catalog. We evaluated each provider's most complete published offering, including its own add-ons, and ours with the same rigor. We used only public information (official websites, documentation, and press releases) reviewed as of September 29, 2026.

What each status means

Offers it: the provider delivers it, operates it, and is accountable for it within its service, wherever the technology comes from. Add-on: available at an additional cost. Partial: limited scope, or requires another contract or another operator. No public evidence: no public information confirms it at the time of review; this does not mean the provider doesn't offer it. Not part of its published offering: its documentation indicates it is not included. Your team provides it: with a tool, that capability depends on your staff, your shifts, and your response times, not on the provider. When in doubt between two values, we chose the more conservative one.

How we make corrections

A provider may offer something it doesn't publish: confirm it directly with them. If you see outdated or incorrect information, write to us through our contact form and we'll correct it in the next version. We review this comparison every quarter and whenever a provider's published offering or our catalog changes.

Evaluated for Vicarius: Vicarius vRx (full platform: vPatch, vShield, vScore, vScript and ScriptAI, vComply, and vIntelligence; multi-tenant IT provider edition), reviewed Sep 29, 2026

Evaluated for TecnetSOC: TecnetSOC in its most complete offering (Compliance plan, with the TecnetProtect and TecnetGRC add-ons), platform catalog soc.catalogo.tecnetone.com and tecnetone.com/servicios/soc-as-a-service, reviewed Sep 29, 2026. Same standard as the others. Add-ons at an additional cost count as part of the offering, just like the other providers' own add-ons.

1. customer-portal.vicarius.io/vrx-for-mssps (Differences you notice day to day)
2. www.vicarius.io/articles/vrx-for-incident-response (Differences you notice day to day)
3. www.vicarius.io/ (Differences you notice day to day)
4. www.vicarius.io/features/patch-management (Differences you notice day to day)
5. [www.vicarius.io/articles/from-vulnerability-management-to-compliance...](https://www.vicarius.io/articles/from-vulnerability-management-to-compliance) (Differences you notice day to day)
6. www.vicarius.io/features/vrx-analysis (AI agents that investigate and filter alerts...)
7. www.vicarius.io/solution/vulnerability-remediation (Human Gate: a person approves every...)
8. customer-portal.vicarius.io/vrx-user-guide (Leadership reports in Spanish and in business...)
9. www.vicarius.io/trust (Independent certification of operations (ISO 27001...))
10. www.vicarius.io/articles/virtual-patching-legacy-software (Advanced protection on every device (EDR/XDR)...))
11. customer-portal.vicarius.io/assets (Unified asset and software inventory)
12. [www.vicarius.io/articles/cvss-vs-epss-vs-kev-which-score-actually-matters...](https://www.vicarius.io/articles/cvss-vs-epss-vs-kev-which-score-actually-matters) (Vulnerabilities prioritized by severity...)
13. www.vicarius.io/articles/what-is-vulnerability-remediation-in-2026 (Closure verification: the scanner confirms...)
14. www.vicarius.io/solution/continuous-exposure-management (External attack surface: what your company exposes...)
15. www.vicarius.io/pricing (Per-device pricing, with plans that stack)
16. www.g2.com/products/vrx-by-vicarius/pricing (Free plan to get started)
17. www.capterra.com/p/201047/vRx/ (Free trial in your real environment)
18. [www.vicarius.io/solution/vicarius-vrx-for-teams-secops-and-vulnerability...](https://www.vicarius.io/solution/vicarius-vrx-for-teams-secops-and-vulnerability) (Available under your IT provider's brand)

Sources and date. This comparison is informational and is prepared by TecnetOne so you can compare, capability by capability, what TecnetSOC includes versus the most complete published offering of each provider mentioned. The list of capabilities is TecnetOne's own catalog and may not include every feature of each provider. We used only public information (official websites, technical documentation, and press releases) reviewed as of September 29, 2026; version 2026.09, reviewed quarterly. "No public evidence" means that no public

information confirms it at the time of review, not that the provider cannot offer it in another way: confirm every detail directly with them. The sources for each data point are in each provider's individual comparison, linked at the bottom of the table.

Trademarks. Third-party names and trademarks belong to their respective owners and are used only to identify them and for informational comparison. None of these providers is affiliated with TecnetOne or sponsors or endorses this document.

TecnetSOC scope. Backup and the compliance platform (TecnetGRC) are add-ons at an additional cost. Our times are service targets for notification and investigation start, not for resolution (critical: 30 minutes, as a target). Patching is subject to the maintenance windows agreed with you and to the applications included in your profile. Compliance is delivered as readiness and evidence, not as certification. TecnetSOC is a TecnetOne service, with ISO/IEC 27001:2022 certified operations, available directly or through your IT provider.



A SOC that speaks your language.

[See outdated or inaccurate information? Write to us and we'll correct it.](#)